

1 DANIEL G. BOGDEN
United States Attorney
2 MICHAEL CHU
Assistant United States Attorney
3 333 Las Vegas Boulevard South, Suite 5000
Las Vegas, Nevada 89101
4 Telephone: (702) 388-6336

5
6 **UNITED STATES DISTRICT COURT**
7 **DISTRICT OF NEVADA**

8 -oOo-

9
10 UNITED STATES OF AMERICA,) Case No. 2:11-mj-00724-VCF
11 Plaintiff,)
12 vs.) **SEALED COMPLAINT**
13 KATHERINE M. KAPLAN,)
14 Defendant.)
15

16 BEFORE the United States Magistrate Judge, Las Vegas, Nevada, the undersigned complainant being
17 first duly sworn, deposes and says:

18 **COUNT ONE**
Conspiracy to Commit Computer Fraud

19 From in or about June 2010 to in or about March 2011, in the District of Nevada and
20 elsewhere,

21 **KATHERINE M. KAPLAN,**
22 defendant herein, did knowingly and willfully combine, conspire, and agree with others known and
23 unknown to commit the crime of computer fraud, that is, the defendant and others did knowingly
24 and with intent to defraud access a protected computer, exceeding their authorized access and by
25 means of such conduct furthered the intended fraud and obtained something of value, specifically,
26 confidential customers leads and other confidential trade secrets of Selling Source, LLC, in

1 violation of Title 18 U.S.C. Sections 1030(a)(4) and (c)(3)(A), all in violation of Title 18, United
2 States Code, Section 371.

3 **Affidavit in Support of Complaint**

4 Complainant, Special Agent Scott Baugher of the Federal Bureau of Investigation, being
5 duly sworn, states the following as probable cause to support the above allegations:

6 **Summary**

7 Starting no later than June 2010 to at least March 2011, a group of former Selling Source,
8 LLC ("Selling Source") employees (including Katherine Kaplan), and their allies conspired with
9 Kim Baxa, a current Selling Source employee to obtain money and property by means of
10 materially false and fraudulent pretenses, representations and promises, by stealing Selling
11 Source's valuable trade secrets. These secrets included hundreds of thousands of customer leads,
12 sensitive contracts and pricing information, and documents discussing future ad campaigns. The
13 aggregate value of the customer lead information alone appears to be in the tens of millions of
14 dollars. The conspirators intended to exploit these trade secrets by forming a rival company that
15 would compete with Selling Source. The FBI seeks a warrant from this Court for the arrest of
16 Katherine M. Kaplan.

17 **Introduction**

18 1. I am a Special Agent with the Federal Bureau of Investigation, currently assigned to
19 Las Vegas, Nevada. I have been employed as a Special Agent of the FBI since June 2004. Over
20 the course of my employment with the FBI, I have investigated a wide variety of matters, including
21 cases involving computer intrusions, Internet fraud, counterterrorism, and bank robberies. During
22 the course of my FBI employment, I have served numerous search warrants on both E-mail
23 accounts and physical locations. Prior to my employment with the FBI, I was employed as the
24 chief technology officer of a web development and Internet hosting company where I gained
25 extensive experience relating to Internet communications. I hold a Bachelor's of Business
26 Administration degree in Computer Information Systems. Currently, I am assigned to the

1 Cybercrimes FBI squad in Las Vegas, and have substantial experience investigating computer-
2 related criminal violations.

3 2. The information contained in this affidavit is based on, among other things, my
4 personal knowledge and observations during the course of this investigation, information
5 conveyed to me by the divisions of the FBI, the public, other government agencies and officials,
6 other law enforcement agencies and officials, and my review of records, documents and other
7 evidence obtained during this investigation.

8 3. Due to my training, my experience and this investigation, I am also familiar with
9 the internet, online service providers such as Dropbox, Yahoo! and Google (and others), and the
10 manner in which criminals use the internet and computers to further their schemes. Moreover,
11 references to my experience include my discussions with other law enforcement officers who also
12 have such experience.

13 4. At all times during the investigation described herein, I have acted in my official
14 capacity as a Special Agent of the FBI. Since the Affidavit is being submitted for the limited
15 purpose of securing an arrest warrant for Katherine M. Kaplan, I have not included each and every
16 fact known to me concerning this investigation. I only set forth the facts that I believe are
17 necessary to establish probable cause for the issuance of this arrest warrant.

18 **The Person to be Arrested**

19 5. Katherine M. Kaplan is a Caucasian female, believed to be residing in Ecuador,
20 with a former residence in Henderson, Nevada. As will be more fully described later, Kaplan is a
21 former Selling Source employee and contractor.

22 6. The Affidavit is in support of an application for an arrest warrant for Katherine M.
23 Kaplan, who I have probable cause to believe did violate, among other statutes, Title 18, United
24 States Code, Sections 371 (conspiracy to commit computer fraud – exceeding authorized access)
25 (the "Subject Offense").
26 . . .

7. I understand that the elements of a violation of 18 U.S.C. § 371 (conspiracy) are as follows:

First, beginning in or about June 2010, and ending no earlier than in or about March 2011, there was an agreement between two or more persons to commit at least one crime as charged;

Second, the defendant became a member of the conspiracy knowing of at least one of its objects and intending to help accomplish it; and

Third, one of the members of the conspiracy performed at least one overt act on or after June 2010 for the purpose of carrying out the conspiracy, with all of you agreeing on a particular overt act that you find was committed.

8. In turn, I understand that the elements of a violation of 18 U.S.C. § 1030(a)(4) (computer fraud – exceeding authorized access) are as follows

First, defendant or another co-conspirator knowingly exceeded authorized access to a computer used in or affecting interstate commerce or communication;

Second, a co-conspirator did so with the intent to defraud;

Third, by exceeding authorized access to the computer, the co-conspirator furthered the intended fraud; and

Fourth, the co-conspirator by exceeding authorized access to the computer obtained some thing of value.

Facts

Introduction

9. Based on my investigation, I submit there is probable cause to believe that Katherine (also known as “Kathy” or “Kat”) Kaplan, a former Selling Source, LLC, consultant, conspired with Kim Baxa, a current Selling Source employee, to steal Selling Source’s data and sell it to Selling Source’s rivals. The rivals initially consisted of Curtis Pope, Charlie Wurm, and others. Later, Kaplan and Baxa had a falling out with Pope (and by extension, Wurm). At that point Kaplan and Baxa began to work on their own (with others), leaving Pope and Wurm to form new partnerships with others and begin working on their own as well.

► ● ■

• • •

1 **Background regarding Selling Source, LLC, and its subsidiaries**

2 10. On August 8, 2011, I met with representatives of the victim, Selling Source, LLC.
3 According to them, Selling Source is a company based in Las Vegas that is one of the largest
4 digital marketing companies in the United States. Selling Source primarily buys, generates and
5 markets leads for payday loans. This information is both valuable and time-intensive to generate.
6 For example, according to Selling Source, the company purchases leads from third-party affiliates
7 for approximately \$44/lead, and is able to sell them for \$55/lead. (Notably, this case involves
8 hundreds of thousands of stolen records, so, under that valuation, the stolen data is worth tens of
9 millions of dollars.)

10 11. Selling Source owns several subsidiaries including Optimized Contact Solutions
11 (OCS), for which Baxa and Kaplan worked; and Partner Weekly, dba Money Mutual (for
12 convenience, I may refer to these any or all of these entities as Selling Source). Selling Source
13 creates marketing campaigns for the payday lending businesses: Money Mutual is an example of
14 one such campaign. Selling Source's Money Mutual campaign consists of E-mail, direct mail, and
15 television advertisements, some of which feature Montel Williams. When customers respond to
16 the ads, their information is collected, and they are matched to a Selling Source affiliated lender
17 (Selling Source does not itself lend money). The lenders pay Selling Source for each customer
18 lead. Even after the loan is fulfilled, there is still value in the data Selling Source has collected
19 because customers who have previously applied for payday loans are more likely to apply again.

20 12. OCS was a direct mail company. According to Selling Source employees, OCS
21 mailed all the consumers that completed loan applications on Selling Source's websites. OCS had
22 access to all of Selling Source's data as a result because it needed to send files to the mail houses
23 that did fulfillment.

24 13. Most of the co-conspirators addressed in this affidavit are former (or current)
25 employees of Selling Source or its affiliates. Kim Baxa is currently Director of Operations for
26 Optimized Contact Solutions. Kathy "Kat" Kaplan is a former vice-president of marketing of

1 Optimized Contact Solutions. Curtis Pope formerly ran a call center for Selling Source. Charlie
2 Wurm is a former network administrator for Selling Source, where he supported the company's
3 network and call center.

4 **On June 28, 2010, Kat Kaplan E-mails to Curtis Pope data stolen from Selling Source**

5 14. Previously, I obtained warrants to search KatKaplan@msn.com and
6 CP1234@me.com. As further described below, my review of the contents of these E-mail
7 accounts show that they belonged to Kat Kaplan and Curtis Pope.

8 15. Around June 28, 2010, Kaplan sent an E-mail from her account at
9 katkaplan@msn.com to Curtis Pope (cp1234@me.com) with the message simply being, "Attached
10 is a zip file of the creatives. Talk to you tomorrow." Attached to the E-mail was a file called
11 "creatives.zip," which I reviewed.

12 16. "Creatives.zip" appears to contain data stolen from Selling Source, LLC, according
13 to Selling Source, LLC's President Glenn McKay to whom I showed this file. (Generally, a .zip
14 file is a way to bundle files together in one .zip archive, so that they can be sent as one file.)
15 Specifically, "creatives.zip" mostly related to Selling Source's subsidiary, Partner Weekly, and the
16 sale of payday lending leads to lenders. McKay told me "creatives.zip" would be particularly
17 valuable to anyone wishing to compete with Selling Source, because the file included trade secrets,
18 such as, among other things, pricing information relating to the sale of leads to a particular
19 company.

20 17. By June of 2010 Kaplan was no longer vice-president of marketing, but she still
21 worked for Selling Source, LLC, as a contractor, training her replacement and helping to ensure
22 everything stayed on budget during her transition out of the company. Kaplan's contract with
23 Selling Source, LLC ended in June 2010, a fact that severely restricted Kaplan's access to Selling
24 Source data. Therefore, I believe that Baxa joined the conspiracy as a result of Kaplan likely
25 recruiting Baxa in order to maintain access to Selling Source's data after Kaplan left.

26 . . .

1 **On June 29, 2010, Kaplan E-mails more stolen data to Pope**

2 18. Around June 29, 2010, Kaplan sent another E-mail to Pope. The message read
3 simply, "Sorry guys... I sent the wrong files last night. Please forward to Gordon." Kaplan's E-
4 mail contained four zip archives, all of which appear to me to belong to Selling Source.

5 19. For example, one archive contained a file named
6 OCS_Montel_Control_062910b.zip, which contained a PDF file that when opened appeared to be
7 a mailer design for Selling Source's Money Mutual ad campaign, with a picture of Montel
8 Williams on it. (As noted above, Money Mutual is a payday lending marketing campaign
9 belonging to Selling Source.) Moreover, the file name also suggests its origin:
10 OCS_Montel_Control_062910b.zip refers to Optimized Contact Solutions (OCS), the Selling
11 Source subsidiary for which Baxa and Kaplan worked, and the ad campaign featuring Montel
12 Williams. This ad campaign runs in states outside Nevada, and its goal, according to Selling
13 Source, is to generate leads for payday loans. Some of these leads, thus, come from outside
14 Nevada and thus, Selling Source's computers (to which Baxa and Kaplan conspired to exceed
15 authorized access) are computers that affect interstate commerce.

16 20. Another file was called "SS_6x9_041610_Final.zip." I believe the "SS" part of the
17 file name likely stands for Selling Source. The archive contained an identically named PDF that
18 appears to be a mailer design for CashLoanNetwork.com, which, according to Selling Source
19 President Glenn McKay, is another Selling Source ad campaign for payday loans.

20 **Baxa (and Kaplan) were well aware that company data was required to be kept confidential**

21 21. Baxa, as noted above, works for Selling Source's subsidiary, Optimized Contact
22 Solutions (OCS). OCS sends direct mail marketing materials to individuals who fill out loan
23 applications, as a result of various Selling Source marketing campaigns. Baxa's job title at OCS is
24 "Director of Operations."

25 22. Baxa's employment agreement required her to keep company information
26 confidential. Under Baxa's employment agreement, Baxa agreed to keep confidential "all

1 information obtained through [her] work related duties that is not general public knowledge.”

2 Notably, Baxa acknowledged that her employer and its clients had “business and technical
3 information which they keep in confidence” and that the goodwill and competitive ability of her
4 employer depended on keeping its information confidential. Thus, Baxa agreed to “not release,
5 use or disclose” such information except with the prior written permission of her employer.

6 23. Similarly, Kaplan agreed to keep confidential, “all information obtained through an
7 employee’s work-related duties that is not general public knowledge ... provided to her by
8 Optimized Contact Solutions, Ltd. or its clients, excepting only such information as is already
9 generally known to the public, and that she shall not release, use, or disclose the same except with
10 the prior written permission of Optimize Contact Solutions, Ltd.”

11 24. This policy was echoed in the Policy Statement for Information Security, which was
12 attached as Exhibit 1 to the employment agreement. I reviewed this Statement, and it emphasized
13 that “to meet its operational, financial, and legal responsibilities, the Company must protect its
14 proprietary information and intellectual property.” It also reminded employees that “Trade secrets,
15 all documents marked confidential, and any sensitive business information disclosed to an
16 employee must not be divulged or used in non-Company-related business.”

17 25. Baxa knew that she was prohibited from uploading company data. I reviewed her
18 employer’s “Mandatory IT Policies.” Under these policies, “Uploading or transferring any
19 company network data to unauthorized or unapproved websites or individuals is strictly prohibited.
20 (This data includes all files and directories residing within company servers or connected to the
21 company network.)” Kaplan also signed an IT use policy where she agreed to the same terms.
22 The policy that Baxa signed also prohibited her from “accessing data of which the employee is not
23 an intended recipient or logging into a server or account that the employee is not expressly
24 authorized to access, unless these duties are within the scope of regular duties.”

25 26. Further, Selling Source, according to Chief Technology Officer Scott Barbour,
26 expends considerable time, money and effort on security measures to protect its confidential data

1 from disclosure to third parties. For example, access to Selling Source's computers is governed by
 2 a layer of passwords; almost all of the data discussed herein is protected by a second layer of
 3 passwords for that particular department where the data is stored; and only certain authorized
 4 employees are granted access to this data. Moreover, Selling Source's offices are restricted to only
 5 authorized employees and governed by a PIN access to a keypad. Employees who work from
 6 home must log in to Selling Source's computers using a "secure ID token verification system."

7 27. Finally, to ensure that employees are not stealing company information, Selling
 8 Source entered into employment agreements with Baxa and Kaplan. Under this employment
 9 agreement, Baxa and Kaplan acknowledged their internet, E-mail and computer use enjoyed "**NO**
 10 **EXPECTATION OF PRIVACY**" (emphasis in original). They also agreed, among other things,
 11 that "OCS, due to the nature of OCS business and the interest in protecting proprietary
 12 information, shall monitor employee use of the Internet, email (whether email from a company or
 13 private account so long as the email is accessed from a company computer in the case of the
 14 latter), OCS computers (including key strokes, web surfing, ICQ etc.), OCS phone system and all
 15 other technology utilized by OCS to carryout company functions." Baxa and Kaplan signed and
 16 acknowledged similar policies in Selling Sources' "Mandantory IT Policies."

17 **On August 6, 2010, Kim Baxa E-mails stolen data to Kaplan**

18 28. Despite these restrictions, Baxa has, starting no later than August 2010, been
 19 working with Kaplan to steal Selling Source data, and sell it to Pope, Wurm and others.

20 29. On August 6, 2010, Baxa (kimi706@aol.com)¹ sent an E-mail to Kaplan
 21 (katkaplan@msn.com), which was an essentially blank message, with four file attachments. These
 22 files all related to Selling Source's Money Mutual campaign featuring Montel Williams. The files
 23 contained direct mail and other advertising samples for the campaign. This is significant, because
 24 this file suggests that co-conspirators such as Pope, Wurm and others intended to use data stolen
 25

26 ¹ I previously obtained a warrant to search kimi706@aol.com, and from its contents, I believe it was used by Kim Baxa. Some of these contents are described herein.

1 from Selling Source to replicate Selling Source's Money Mutual payday lending product.

2 30. Money Mutual appears to be well-known in the payday lending industry. I base this
3 on the fact that, as later explained, Jason Rudolph, when pitched by Pope to participate in his
4 scheme, recognized the similarity to the Money Mutual campaign, and knew that it belonged to
5 Selling Source. He was, in fact, so concerned that he contacted Selling Source directly and warned
6 it of a possible theft of data and other materials.

7 **On November 16, 2010, Baxa demands payment before she sends any more "prime files"**

8 31. On November 16, 2010, Baxa complained to Kaplan about her lack of payment.
9 Her E-mail stated, "It is now 3 weeks past...im tired of the games and saying same shit. I have
10 given 550k and all that has been paid is 25k. I want the original 10k each and when i see 30k in my
11 acct we can revisit sending another thing." I believe that "550k" refers to the number of stolen
12 customer/sales leads sent to Pope. I believe that Baxa's reference to "25k" refers to payments
13 already received from Pope; "10k each", and "30k" refers to payments she hopes to receive from
14 Pope.

15 32. The next day, on November 17, 2010, Baxa sent another E-mail to Kaplan
16 demanding payment before she sends any more "prime files" to Pope (via Kaplan):

17 I want consistency and i want the guy to stick to his word.
18 The files i give are prime files. He knows that. I want to be
19 fairly compensated for it. I gave 550 k records n the cost is
20 around .03 each with what has been paid out. I want payment
21 for the last file of 269k and then i want payment BEFORE i
22 send another one.

23 [...]

24 I am pissed that he expects things yesterday. he can call it
25 holding hostage and he is right. i am not jumping anymore.

26 Basically when we get a real amount for what he has
received and more for the next thing i will then send it on my
time.

27 33. Notably, Baxa's E-mail also discussed proceeding on a separate front, so she and
28 Kaplan could "get paid for the data" by a different customer, "phillip."

1 As for phillip we can still move forward. I doubt he is
2 working with him n even if he is it is two separate things.
3 Maybe we would even get paid for the data.

4 **On November 18, 2010, faced with Baxa's ultimatum, Pope quickly responds with a \$20,000
5 payment; all parties use intermediaries to disguise the payment**

6 34. Pope paid Kaplan (who, in turn, paid Baxa); but the manner in which they did this
7 shows their consciousness of guilt because they all tried to conceal the payments by using
8 intermediaries.

9 35. On November 18, 2010, the day after Baxa sent her ultimatum, Pope paid Kaplan
10 \$20,000. I infer this from the fact that Pope (cp1234@me.com) received a wire transfer
11 confirmation from "Angelo" (floridan100@gmail.com), which showed that \$20,000 was
12 transferred to the bank account of Karen McChesney (Kaplan's sister) on or about November 18,
13 2010.

14 36. Kaplan then E-mailed Baxa (kimi706@aol.com) asking, "How would you like it?"
15 (i.e., how would Baxa like to be paid?). Baxa responded the following day, directing Kaplan to
16 send it to "Donna's" account. I believe based on this investigation that "Donna" refers to Donna
17 Finerty, Baxa's then live-in girlfriend.

18 37. A few days later, on November 23, 2010, Kaplan E-mailed Baxa with the subject,
19 "Did Karen get you your stuff?" The next day, Kaplan sent Baxa another E-mail which said,
20 "Should be there now."

21 38. I believe these E-mails show that Kaplan paid Baxa by conspiring to cause
22 McChesney to launder money on their behalf, in order to hide the source of the payments (Pope),
23 and the reason they received them (for the data stolen from Selling Source, LLC). Notably, the use
24 of intermediaries shows that all of the individuals involved are laundering the funds sent between
25 them in order to attempt to disguise their association and prevent the discovery of their illegal
26 activity.

1 At the same time, on November 18, 2010, Pope and Wurm continued to ask for more stolen
2 data from Kaplan and Baxa

3 39. On November 18, 2010, Wurm (charlie.wurm@proacquire.com) sent Kaplan
4 (katkaplan@msn.com) an E-mail. The subject of the E-mail was, "Getting close & "The Big File"
5 Request." The E-mail read (in part): "Kathy, Curtis wanted you to see the E-mail thread below
6 regarding movement and development on the lead system. He also asked that I request "the big file
7 with all of the incompletes" from you. I assume you know what he means."

8 40. Kaplan then forwarded this message to Baxa (kimi706@aol.com) the same day
9 (November 18, 2010), telling her, "Kim - Can you send me your phone number? I want to talk to
10 you about this. Thanks. I will not be home until Dec 10th. -Kathy." (The timing is consistent
11 Baxa's ultimatum: as of November 18, 2010, Baxa had not yet received payment.)

12 41. On November 19, 2010, Baxa (kimi706@aol.com) provided her phone number to
13 Kaplan (katkaplan@msn.com), and then advised:

14 The big file takes about 2 hours for for [sic] just ones days
15 worth of data - then when I dedupe - it goes from 500k to
16 20k. I need to mess with my code to figure out how to speed
17 it up. These are the fails I am talking about. If I could just do
18 name and address no other stuff it would be faster probably.
19 Call me when ever.

20 42. In response, Kaplan asked Baxa, "Would it help if Jeff helps you with the
21 deduping? Or do you need to do it online?" I believe that Kaplan is asking if Baxa needs to be at
22 Selling Source, LLC's offices and connected to their system in order to remove duplicate records.
23 (I am currently unsure who "Jeff" is.) Baxa replied, "Has to be done here. My machine crashes. So
24 it will take time." This is another example that shows that Kaplan knows the data is being
25 provided by Baxa, an employee of Selling Source, LLC.

26 43. On November 20, 2010, Baxa then E-mailed Kaplan: "I spoke to magoo...he called.
Same old song and dance. I told him i should have something wed. Im still waiting for karen. She
said something about ur phone. First data should be taken care of. I sent ryan a text the other day
for payouts."

1 44. This message is significant for several reasons. First, I believe "magoo" is Pope,
 2 based on other E-mails I have seen. Second, Baxa appeared ready to resume sending Pope files
 3 now that Kaplan had received money from Pope (and thus, Baxa was more likely to receive
 4 payment from Kaplan). Third, "Ryan," who I believe to be Kaplan's son Ryan Johnson, appears to
 5 be making "payouts" to people, again likely to conceal the source of the funds generated from the
 6 illegal activity.

7 **On November 22, 2010, Baxa starts using E-mail account kdb_40@yahoo.com, and uploads**
 8 **two files of stolen data**

9 45. Baxa started using a new E-mail address (and a code name, "shortstop"),
 10 presumably to conceal her role from outsiders. On November 22, 2010, Baxa (using
 11 kdb_40@yahoo.com) sent a message to Pope (cp1234@me.com) and
 12 (Kaplan(katkaplan@msn.com)), with the following text: "Shortstop here. You can send any E-
 13 mails to this E-mail. I will have two things for you on Wednesday as discussed. Have a great day!"

14 46. It later becomes clear through both messages sent to and received by
 15 kdb_40@yahoo.com, that the account holder is Baxa. Further, I believe the two things promised
 16 are files belonging to Selling Source.

17 47. The same day, Pope responded to Baxa's message saying, "It's beginning to look a
 18 lot like Christmas!!!" Pope told Kaplan, "Thank you for always backing me partner." I believe
 19 this E-mail shows that all of the parties on the E-mail knew what was going on, to wit, their plan
 20 was being carried out, and that Kaplan had successfully convinced Baxa to continue stealing
 21 Selling Source's data.

22 48. Later the same day, Baxa (kdb_40@yahoo.com) notified Pope (cp1234@me.com),
 23 Kaplan (katkaplan@msn.com): "They are uploaded." I believe this refers to the two files Baxa
 24 previously promised to upload to a third party's FTP website.

25

26

From December 2010 to March 2011, Baxa (and Kaplan) continue to provide stolen data to Pope, Wurm, and others

49. From December 2010 to March 2011, Baxa (and Kaplan) continued to provide stolen data to Pope, Wurm, and others.

50. For example, on December 14, 2010, Kaplan (katkaplan@msn.com) sent four E-mails to a third party, cc'ing Pope (cp@ireason1.com)² The subject of each message was "File [x] of 4." Each message contained a zip archive, which were named for months July, August, September, and October. Each file contained a spreadsheet with Selling Source, LLC data, including the full name, address, phone number, and E-mail address. The spreadsheets also contained a "URL" field, which listed what I believe to be the web site the customer used to submit their application. I checked the first seven unique URLs, which Glenn McKay of Selling Source told me all belonged to one of their affiliates. In addition, I saw that some of the referring URLs were related to Money Mutual, which I know is owned by Selling Source.

51. Later that day, the third party replied to Kaplan and cc'ed Pope, informing Kaplan that he (the third party) had received the files and that "everything looks good."

52. McKay told me that Selling Source purchases those leads from third-party affiliates for approximately \$44/lead, and is able to sell them for \$55/lead. In total, the spreadsheets contained over 272,000 customer records for July, over 303,000 records for August, over 272,000 records for September, and over 273,000 records for October. Thus, the value of all of the data contained in just those four spreadsheets appears to exceed \$49 million (1.12 million customer records x \$44 each).

. . .

. . .

. . .

² Pope also uses cp@ireason1.com; I know this because in cp1234@me.com is an E-mail from "Curtis Pope <cp@ireason1.com>."

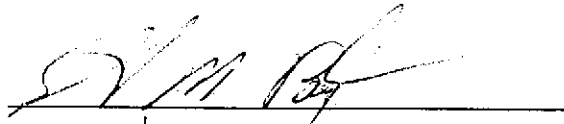
1 **By March 9, 2011, Kaplan and Baxa have a falling out with Pope – but offer to continue the**
2 **scheme with a third party**

3 53. After March 9, 2011, Kaplan and Baxa no longer communicate with Pope. It is at
4 this point that the criminal enterprise appears to fork, with Kaplan, Baxa, and others on one side,
5 and Pope, Wurm, and a number of others on the other.

6 54. Based on the foregoing information, I submit there is probable cause to arrest
7 Katherine M. Kaplan for the above-listed violations, which are incorporated herein by reference.

8 **Sealing Application**

9 I also respectfully move this Court for an Order sealing this affidavit and complaint until such time
10 as the Court (or another Court of competent jurisdiction) shall order otherwise. I submit it is
11 necessary for this document to be sealed in light of the fact that it makes reference to information
12 regarding an on-going investigation. I submit that disclosure of this information might jeopardize
13 the investigation. I submit that the United States' right to secrecy far outweighs the public's right
14 to know.

15
16 
17 Scott Bauger, Special Agent
18 Federal Bureau of Investigation

19 SUBSCRIBED and SWORN to before me
20 on November 2, 2011.

21 
22 UNITED STATES MAGISTRATE JUDGE
23
24
25
26